Testimony and Statement for the Record of
Dr. Jason Catlett
President and CEO, Junkbusters Corp.
Visiting Scholar, Columbia University Department of Computer Science
on
Privacy Protection
before the
Committee on Commerce, Science, and Transportation
U.S. Senate

May 25, 2000

[Note: These comments were written after seeing the FTC's report. They replace an earlier version.]

My name is Jason Catlett, and I am President and CEO of Junkbusters Corp., a for-profit dot com company working to promote privacy.
I'm very grateful to the Senate for this opportunity to discuss with you how to protect privacy in the Internet age.

I came to this country from Australia eight years ago to join the computer science research staff at AT&T Bell Laboratories.
Since I founded Junkbusters in 1996, the company has published advanced software and provided services and information to help people defend their own privacy. These resources have been used by hundreds of thousands of Americans.
Based on feedback from people across this country, and my own investigations, I have been led to the conclusion that technical solutions to
the challenges of privacy will not prevent the death of American privacy online.
It is clear to me that legislation is appropriate and necessary to protect privacy on the Internet.

My work in marketing and databases at AT&T Bell Labs was governed by strict laws
to protect the privacy of telephone subscribers. The Internet still has few corresponding laws,
so companies are engaging in practices that would be regarded as unacceptable and illegal on a phone network.

Collectively, this commercial
surveillance is having the tragically perverse consequence of
scaring off consumers from the entire medium rather than attracting them to a particular site.
The Harris/Business Week polls and many others since 1998
have found
that fear for privacy is a major or primary
reason consumers give for not going online, and for not participating in ecommerce.
Their 2000 poll showed a strong majority of Americans favoring new privacy legislation.

Forrester Research,
a highly regarded firm of technology analysts whose reputation has been built by providing accurate research and advice to companies,
has harshly criticized the poor standards of privacy protection online, finding in September 1999 that 90 percent of Web sites fail to
comply with basic privacy principles.
Forrester called most privacy policies ``a joke'' and concluded that ``the vast majority
of such policies, like those of the Gap, Macy's and JC Penney, use vague terms and legalese that serve to protect companies and not individuals."
These are not the words of some bleeding heart privacy advocate, but of hard-nosed analysts working for a company whose long-term success heavily depends on understanding and promoting
the growth of Internet commerce.
In October 1999 Forrester published a report finding that ``Nearly 90% of online consumers want the right to control how their personal information is used after it is collected.
This desire for online anonymity cuts across consumers from a broad range of demographic backgrounds, including gender, income, and
age. Surprisingly, these concerns change very little as consumers spend more time online." It is not ignorance that is causing Americans to worry. It is a rational assessment of the lack of
control over their personal information,
and the paucity of recourse available to them if it is misused.

This privacy problem will not go away by itself because the economic incentives of individual companies work against it.
As an example, providing customers with an opt-out from a list of phone numbers being sold to telemarketers
means both forgoing future revenue and incurring a capital cost to set up an opt-out system.
Companies can ill afford to unilaterally jump ahead of their competitors, even though the sums of money are minor compared to the increase in participation
that would result from a market where privacy rights are widely respected. The idea that consumer demand will force companies to offer privacy
protections is naive and simply not supported by empirical evidence in surveys. What company is going to produce advertising copy
like the following? ``Buy books from us and we will give you a choice in whether we sell your phone number to telemarketers."
As Commissioner Anthony wisely observed in a statement Monday, legislation of the kind recommended by the FTC
``would reward those sites that have offered
real privacy protections and require all others to meet basic privacy standard."

We are facing a tremendous loss of both economic opportunity, and of our fundamental human right to privacy.
The only way to stop this tragedy is to require
all companies to respect the privacy of their customers and prospects. And that is an entirely proper

thing for the federal government to do.

On the Internet this loss is particularly acute, but is obscured by technical complexity.
Let me describe one example by analogy.

Online advertisers build up profiles based on where people go, what they look for, and how they behave on the Net.
Imagine if Congress had not passed laws to protect the privacy of telephone users.
The headlines would be full of the kind of privacy horror stories we see today about the Internet.
We might see a telco that I will fictionally name Orwell Long Distance using
speech-recognition technology to spot keywords in your conversations
with businesses in order to target you with more interesting telemarketing calls. OLD might look up the yellow pages categories of the numbers you frequently call, and sell that information to junk mailers to decide
the kinds of catalogs you're less likely to throw away. This sounds absurd to us now, but
on the Web, equivalent practices abound, unrestrained.

Banner ad companies get to see the specific Web pages people visit, plus the keywords they type into search engines and other forms.
They track individual PCs using unique identifiers called ``cookies" placed on Web browsers.
Most people haven't heard these companies' names,
but some of them have started identifying people by name. Large profiles that were previously gathered with just an anonymous identifier
are being linked to a street address, and phone number, and email address.

If Orwell Long Distance were unencumbered by present phone privacy laws, its lobbyists would
be telling Congress that any attempt to restrict the free flow
of information on the international phone system would be futile, and could result in the collapse of toll-free ordering.
But you would wisely dismiss that claim and judge that the greater economic good requires that people have confidence that their privacy is protected by law when they do business by phone.

It would be silly to expect consumers to defend themselves from Orwell Long Distance by using
their own voice scramblers and payphones, or indeed technology from OLD itself.
Suppose OLD designed a device that could be held up as a technological solution to the privacy concerns of phone subscribers. The result might be rather like a caller ID box, but in addition to displaying to the name and number of the calling party,
it would indicate the degree of privacy being offered by the various carriers involved in the call. The called party would then supposedly be given "choice" on whether to pick up and speak to her mother for example,
or have her call automatically rejected because it doesn't meet her daughter's privacy "preferences".
This scheme would not protect privacy on the phone,
and its Internet equivalent, P3P, will not protect privacy online.

What people need are simple, predictable standards, not more complexity, just as businesses need simple predictable copyrights.
Both privacy and copyright law accommodate more complex arrangements whenever needed, with the consent of the parties involved.

The comparison with copyright is useful in dismissing many commonly-heard objections to privacy legislation.
``We mustn't impede the free flow of information, so privacy/copyright laws are bad." On the contrary, such laws promote participation in the information economy, by protecting the rights of the participants.
``The Internet is international, so privacy/copyright laws are useless." On the contrary, that is no reason to permit domestic abuses,
and international treaties can be developed.
``Technology changes quickly, so copyright/privacy laws are useless." On the contrary, such laws should be technology-independent;
it is the data that needs protecting, not the means of transmission. ``It's impossible to enforce copyright/privacy laws completely,
so we shouldn't have them."
Of course incidental violations will occur, but
organizations will not base their businesses on piracy/privacy violation, or at least not for long.

Finally, imagine if Recording Industry Association of America were assessing the results of a fictional survey by the Department of Commerce showing that more than 80% of U.S. households do not infringe music copyrights,
and concluding that copyright law should therefore be repealed. Preposterous, the RIAA would say.
Even 95% of households respecting copyright would still leave 5% free to infringe copyrights.
We must have a law. Won't new technology for preventing the unauthorized duplication of CDs provide the answer, a lobbyist against one-size-fits-all legislation might ask? No, the RIAA would say. We need a law,
and we need substantial criminal and civil penalties.
The Digital Millennium Copyright Act of 1998 was Congress's response to this issue.

In general, information technology produces many more opportunities for enabling undesired uses of information than it does for preventing it.
As someone who has personally designed, coded, documented and published privacy-enhancing software,
I would be the last to try to impede such technologies.
The argument by some lobbyists that legislation would dampen technological innovation to protect privacy is specious.
On the contrary, legislation would give companies an incentive to adopt technologies that promote privacy.
Services for assuring anonymity become more valuable in a world
where data protection is required, because anonymity is an infallible way of obviating the misuse of personal information.

The Report and Recommendation of the Federal Trade Commission

The FTC's report has been criticized by some trade associations as understating the level of privacy protection being provided by major Internet sites. I believe exactly the opposite is the case.
Three years of surveys by the Electronic Privacy Information Center plus Forrester's assessment in September provide far stronger evidence that the average site provides substandard privacy.
As an illustration, take the issue of access by consumers to information collected about them.
The Online Privacy Alliance's
spokesperson Christine Varney said in a press release Tuesday that ``There is no agreed-upon standard for access, so how can the
FTC measure it? They can't.'' The answer was on page 23 of the FTC's report: ``With respect to Access, a site received credit if it offers
the ability to review, correct, or delete at least one item of personal information it has collected - oftentimes simply an opportunity to update an email address - without regard to what other information a site may have actually collected or compiled.'' Plainly the FTC can measure access, and they did.
It is significant that the FTC were very easy graders, and yet most sites still failed.
As to the consumer's view of access,
a study in April 1999 by AT&T Laboratories asked respondents about ``importance of whether the site will allow me to find out what info about me they keep in their databases.''
57% replied saying it was very important, 27% somewhat important, 4.2% not important, with the rest not responding.
The FTC's conclusion that legislation is needed to improve consumer confidence in a world where most sites are not providing sufficient privacy is simply unassailable.
What is remarkable is that the majority of Commissioners waited so long before recommending legislation.

The four privacy principles of the Online Privacy Alliance and the FTC
(namely notice, choice, access and security)
are necessary but not sufficient to adequately protect privacy.
Orwell Long Distance for example would post a privacy policy (notice), offer an 800 number where people can opt out of surveillance (choice), let consumers fill out their own change-of-address forms (access),
and deliver all its lists to telemarketers encrypted (security). Missing are affirmative consent
and purpose specificity: not using information gathered for one purpose
(to complete the phone call) for another purpose (to give to telemarketers) without gaining affirmative permission.
These are among the principles endorsed the OECD in 1980 and used as the basis of privacy laws in most developed countries, including recently Canada.

The Consumer Privacy Protection Act of 2000

The Consumer Privacy Protection Act
from Senator Hollings and his colleagues is a landmark work, making a giant strides towards the wide

application of
all these principles,
across technologies and across market sectors,
within a legal framework that will really protect privacy in this country.

The CPPA addresses the problem that privacy policies
have become "moving targets" that are constantly subject to change. Requiring consent for material changes in use
an important part of the principle of purpose specificity. In line with this goal, the requirement for notice might
be waived when the policy change merely narrows the purposes to which information is put, rather than widening them.

The CPPA moves toward addressing
the urgent need for standing institutions that consider privacy and security policy issues not merely in the context of commerce,
but also of government, society and human rights.

Very importantly, the bill provides a private right of action, which is essential if people are to have the means to protect their own interests. Some, but not all enforcement power should vest in
agencies such as the FTC.
Experience with the Telephone Consumer Protection Act of 1991 dispels the scaremongering claim that a vast government bureaucracy
would be needed to curtail privacy violations. The FTC has restricted its enforcement actions to cases of fraud (which are indeed widespread and severe in that industry). State Attorneys General occasionally take action. But it is the precious few individuals who file
suit in small claims court that
have done the most to discourage the telemarketing industry from routinely violating the law.

Finally, to allow further progress,
federal laws should not preempt state law.
A good federal law that allows state Attorneys General sufficient enforcement powers
will reduce the need for new state-specific legislation,
but the states should not be deprived of their traditional role as laboratories of legislative innovation.

Congress now has before it a comprehensive proposal to head off the demise of privacy in this country. It is time for each member of Congress
to decide whether the right to privacy is worth defending,
or whether it should be allowed to lapse into a 20th century memory.

Throughout this nation's history,
the world has looked to the United States as a bastion of liberty, and to its elected governments as defenders of individual rights. Congress now bears a great responsibility for determining

whether that leadership will extend into cyberspace,
and whether the American citizen's right to privacy - a fundamental liberty - will endure into the 21st century.

I appreciate the opportunity to speak before you today. I would be pleased to answer your questions.

[A list of references is available at http://www.junkbusters.com/testimony.html on the Web.]